END-USER COMPUTING WORKPROGRAM

CHAPTER 16WP

(FILE NAME ON DISK # 3 = IS-WP#11.WPD) ***COMMENTS***

This section is intended to determine the adequacy of controls over the use of micro/mini computers in the institution. The degree of control necessary will depend on the reliance the institution places upon micro/mini computers for significant and/or sensitive processing. The remaining steps will be completed only for those areas in the institution, if any, that rely on micro/mini computers for significant and/or sensitive activities. Document any findings, especially those that do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook*.

Tier I

1. Obtain a list of micro/mini computers and the applications processed on them. The list should indicate:

   a. The number and type of micro/mini computers by functional area.

   b. The applications processed on the micro/mini computers, including the software used and its functions.

   c. The institution's estimate of the importance and sensitivity of the information (indicate high, medium, or low).

POLICY AND STANDARDS

2. Determine the adequacy of the institution's micro/mini computer acquisition policy for both hardware and software and whether:

   a. Centralized control and/or purchasing is used.

   b. There is an approved list that must be adhered to (e.g., system or corporate architectural standards).

3. Determine if the institution has an information center/help desk to support the use of micro/mini computers.

4. Determine if written policies and standards exist, and if all employees are aware of them, including:

   a. Micro/mini computer programming.

      1. System development.

      2. Program change control.

b. Program documentation standards.

c. Restrictions on the use of micro/mini computers and the data they contain and/or generate. This should include a prohibition against the copying/-piracy of software.

d. Security.

5. Determine if any data processed is significant and/or sensitive to the institution. If no significant/sensitive data is being processed, proceed to step 10.

STAND ALONE/LOCAL AREA NETWORKS

6. Determine whether micro/mini computers operated in a LAN or stand alone environment are the primary system for any significant and/or sensitive applications. If so, review controls in line with mainframe processing, using applicable sections of the workprogram (e.g., EDP audit, and systems and programming sections).

MICRO/MINI COMPUTERS LINKED TO MAINFRAMES

7. Determine if the micro/mini computers are and/or can be linked to the mainframe processor by dial-up lines or direct connection. Distinguish between dumb terminal and peer to peer or smart terminals.

TRAINING

8. Determine the level and type of training provided for the use of micro/mini computer hardware and software.

DISASTER RECOVERY/CONTINGENCY PLANNING

9. Determine the level of disaster recovery/contingency planning provided for the micro/mini computers, including:

a. Hardware.

b. Software, especially custom software.

c. Off-site storage and/or recreation of the data files.

CONCLUSIONS

10. Review the results of work performed in this section and in sections for planning, audit, and

management. If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

11. Discuss with management:

    a. Violations of law, rulings, regulations, or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

    c. Management's proposed actions for correcting deficiencies.

12. Assign rating (See Chapter 5 for additional information.)

13. Prepare an index of workpapers for this section of the workprogram.

14. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations .

15. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date

_____|_____

Reviewer's Initials

Tier II

Negative responses/determinations should be discussed with management. Their remedy, compensating controls, and your comments must be recorded.

POLICY AND STANDARDS

1. Determine whether policies, procedures, or standards exist for:

   a. Software and hardware acquisition, including:

      1) Cost benefit analysis.

      2) Approved list.

      3) Programming standards.

      4) Change control.

      5) Documentation standards.

      6) Testing.

      7) Ownership of programs, spreadsheets, etc., developed on the institution's time and equipment.

      8) Limitations on in-house software development.

   b. Micro/mini computer use, including:

      1) Use of the output/data.

      2) Restrictions on personal and nonjob related use.

      3) Use of personal equipment and/or software.

      4) Use of unauthorized software.

      5) Modification of the hardware and or software.

      6) Copying or piracy of the software.

      7) File backup.

      8) Confidentiality of data.

2. Verify whether housekeeping procedures have been developed and enforced to provide protection from:

   a. Food.

b. Liquids.

c. Dust, smoke.

d. Magnetic fields.

3. Determine whether procedures have been developed and enforced for:

   a. Backup and off-site storage of critical information.

   b. Inventory control on the hardware software.

4. Determine whether adequate security measures have been established, covering:

   a. Physical security.

      1) Restricted area.

      2) Key locks on the machines.

      3) Removing and securing the data files.

   b. Access controls.

      1) Passwords.

      2) Encryption of data on the disk.

      3) Use of dial-up equipment.

      4) Read only attributes to the files.

5. Proceed to step 10, Tier I.

Examiner | Date

_____|_____

Reviewer's Initials